Acceptable Use of IT Resources with Acknowledgement Form

1. Purpose

   This policy identifies the rules of behavior for state employees and contractors unless authorized by a Department head. These rules describe their responsibilities and expected behavior with regard to information and IT resources usage. All state employees and contractors shall sign acknowledgment indicating that they have read, understand, and agree to abide by the rules of behavior before they are authorized to access any state information or IT resources.

2. Relevant Policies

   a. Information Security Policy
   b. Information Security Policy – Appendix A
   c. Identification and Authentication Policy
   d. Electronic Mail Policy
   e. Social Media Policy
   f. Social Media Guidelines
   g. Social Media Request Form
   h. Mobile Device Management Policy
   i. Mobile Device User Agreement Form

3. Acceptable Uses for IT Resources:

   As stated in 2-2-103(1)(2), MCA,

   > A public officer, legislator, or public employee shall carry out the individual's duties for the benefit of the people of the state.
   >
   > A public officer, legislator, or public employee whose conduct departs from the person's public duty is liable to the people of the state and is subject to the penalties provided in this part for abuse of the public's trust.

   Computer Use

   - Users are individually responsible for assigned computer facilities and IT resources, including the computer, the network address or port, software and hardware. As an authorized State of Montana user of resources, you may not enable unauthorized access to the network by using a State of Montana computer or a personal computer connected to the State of Montana network. Therefore, you are accountable to the State of Montana for all use of such resources.

- Use of State of Montana IT resources shall be for the completion of work-related responsibilities only.
- There is no expectation of privacy while using the State IT resources. All activity can be logged, monitored, and reviewed if abuse is suspected.
- The State is bound by its contractual and license agreements respecting certain third party resources; users are expected to comply with all such agreements when using such IT resources.
- Work-related files and electronic information shall be stored on the State's network to ensure the document(s) are backed up.
- Never attempt to gain access to, disclose, or remove any user ID, information, software, or file that is not your own and for which you have not received explicit authorization to access.
- Users shall not interfere with, encroach on or disrupt others' use of the State's shared IT resources. For example, by
    - playing computer games, streaming video, sending excessive messages, attempting to crash or tie up a State computer.
    - damaging or vandalizing State computing facilities, equipment, software, or computer files.
- Users shall not knowingly transfer or allow to be transferred to, from or within the agency, textual or graphical material commonly considered to be child pornography or obscene as defined in 45-8-201(2), MCA.
- All hardware and software, including downloaded software, shall be authorized, purchased and installed by authorized agency IT staff prior to use.
- Users shall not connect *personally* owned storage media (USB storage devices, external or internal hard drives), including *personal* mobile devices (iPads, Kindles, smartphones, etc.) with the workstation or internal network
- IT resources must not be used for private, commercial, or political purposes.
- Remote Access to the State's internal network must be authorized by supervisor and utilize State approved software.
- Users shall report missing or stolen IT hardware immediately to their supervisor and agency ServiceDesk.
- Users shall notify the ServiceDesk and supervisor in the event of a security incident, if the IT device is acting unusual or if it might be infected by a virus or malware.
- Lock computer system before leaving it unattended, and log off computers at the end of the day.

<u>Passwords</u>

- Develop strong passphrases, minimum of 8 characters. Use a combination of upper and lower case with special and numerical characters,
- Passwords and UserIDs must never be re-used or shared with *ANYONE.*

- Never use personal information for your password (e.g., SSN or date of birth).
- Users must secure their password at all times. Do not write password down (e.g., taped to monitor or under keyboard).
- Link: Identification and Authentication Policy

Internet

Internet usage is provided for the opportunity it gives state employees and contractors to accomplish their job duties.

- The State-provided Internet, Intranet and related services are to be used for the conduct of state and local government business and delivery of government services.
- Agency system administrators, management, and Department of Administration personnel can monitor Internet usage for planning and managing network resources, performance, troubleshooting purposes, or if abuses are suspected.
- Link – see section CP-8: [Information Security Policy – Appendix A (Baseline Security Controls)]

Electronic Mail

- Shall be used for conducting state business. Some general correspondence is permitted, but shall be kept to a minimum.
- Email is considered public record. Employees should have no expectations of privacy.
- Never click on attachments or links to any email from an unknown person or company. Forwarded such suspicious email to DOA-SITSD ServiceDesk immediately (servicedesk@mt.gov).
- State email accounts must not be used to receive emails from non-work related websites.
- Shall not be used to circulate chainmail.
- Shall not send sensitive information to other parties unless appropriately encrypted.
- Shall not send inappropriate materials such as:
    - Sexually offensive, explicit
    - Harassing or discriminatory
    - Gruesome, violent, or sadistic
- Link: Electronic Mail Policy

Social Media

- If authorized, can only be used for work-related purposes
- Work-related communications should be professional and consistent with the agency's mission and the position's responsibilities,
- Links: Social Media Policy, Social Media Guidelines, Social Media Request Form

Mobile Management

- Granting of Mobile Device access to State of Montana IT resources shall be managed by agency IT staff.
- State information managed from a mobile device requires authentication, which must include either a device passcode or user password.
- Passcodes are required to follow the state policy for passwords. This includes biometrics. See previous section for link to Password Policy.
- Jailbroken or "rooted" devices will not be allowed to enroll in the enterprise MDM solution.
- If a device becomes compromised while it is enrolled, state information will be removed and the device will not be allowed access to the State network or State information. Access will not be restored until the device has been wiped or receives a factory reset.
- Links: Mobile Device Management Policy, Mobile Device User Agreement Form

Security Training

- The State of Montana requires all state employees and contractors who access or use state systems receive annual mandatory security awareness training.

Sensitive Information

- Users shall refer to relevant State statutes and their agency's policies for guidance on categorizing State information
- Ensure critical and sensitive information is saved to an appropriate location (i.e. network drives).
- Must not be stored, transferred, or copied to unauthorized locations.
- Use of cloud-based services for Sensitive information is prohibited.
- If transfer is required, shall utilize the State of Montana File Transfer Service when possible.
- Shall only be stored on State-owned portable devices and portable storage if there is a business requirement.
- If non-State-owned portable devices must be used in case of a business requirement, device must be encrypted and password protected for access.
- If position requires access to sensitive information, an Elevated Privileges Acknowledgement form (see attached example) will be signed by designee and approved by management prior to being granted access.
- Shall not be transported outside of the United States on portable devices or portable storage.
- Protect IT devices containing sensitive information (e.g. flash drives, computers, cell phones, etc.) until the device is destroyed or sanitized using approved tools or equipment.
- Report lost, stolen or compromised information to immediate supervisor and agency Information Security Manager.
- Ensure all visitors who have access to facilities that house sensitive information have proper visitor access identification

- [MEDIA SANITATION POLICY LINK]

4. Compliance

Compliance is shown by implementing this Enterprise Acceptable Use of IT Resources as described above. Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this document can be made by submitting an Action Request form. Requests for exceptions are considered by submitting an Exception Request form to DOA_SITSD. Changes to policies and standards will be prioritized and acted upon based on impact and need.

APPENDIX A

(add Agency)
(add Division)

SAMPLE - Rules of System Usage Acknowledgement Form

I _____ have read the **(add Agency and State)** policies and procedures regarding the use of information systems and I agree to comply with all terms and conditions. I agree that all information system activity conducted while doing **(add Agency)** business and being conducted with **(add Agency)** resources is the property of the State of Montana.

I understand that any information system to which I have access, can only be used for its intended purpose. I also agree to avoid the disclosure of any protected information to which I have access.

I understand that **(add Agency)** reserves the right to monitor and log all information system activity including email and Internet use, with or without notice, and therefore I should have no expectations of privacy in the use of these resources.

If my position requires a background check, I understand that the results of this background check can affect my employment. (Identified by agency HR staff)

_____ Yes, this position requires a background check

_____ No, this position does not require a background check.

Signed _____

Position Title _____ Position Number

_____ Date _____

NOTE: This form will be signed by each **(add Agency)** *employee on an annual basis.*

APPENDIX B

(add Agency)
(add Division)
SAMPLE - Rules of System Usage for Users with Elevated Privileges
Acknowledgement Form

A. INTRODUCTION

I _____, understand that I have additional responsibilities given my elevated computer access privileges. I have received training emphasizing the effects my actions can have on all information system activity. Because of these responsibilities, I understand the need for reading and signing this Acknowledgement.

B. FEDERAL AND STATE TAX INFORMATION

I understand the following:

1. I may have access to Federal Tax Information (FTI) and State Tax information as defined in footnote 1 below.
2. That tax returns or tax information disclosed to each user can be used only for a purpose and to the extent authorized by the information manager in connection with the processing, storage, transmission and reproduction of tax returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and providing of other services for purposes of tax administration.
3. That further disclosure of any tax returns or tax information for a purpose or to an extent unauthorized by the information manager for these purposes constitutes a felony, punishable upon conviction by a fine of as much as $5,000, or imprisonment for as long as five years, or both, together with the costs of prosecution (IRC 7213).
4. That further inspection of any tax returns or tax information for a purpose or to an extent not authorized by the information manager for these purposes constitutes a misdemeanor, punishable upon conviction by a fine of as much as $1,000, or imprisonment for as long as one year, or both, together with costs of prosecution (IRC 7213A)
5. That should either unauthorized access or disclosure occur, individually I can be sued by the taxpayer and would be liable for civil damages amounting to a minimum of $1,000 for each act or the actual damages sustained by the taxpayer (whichever is greater) as well as the costs of the court action (IRC 7431).
6. That under Montana law, 15-30-303 MCA, 15-70-209 MCA, 15-70-344 MCA, 15-70-351, MCA, a user cannot disclose or disseminate information contained in a statement required under the fuel tax sections. Making an unauthorized disclosure or unauthorized inspection of information can make the person subject to the progressive disciplinary procedures set out by state law which could include termination from employment.
7. I have received awareness training and understand the policies and procedures for safeguarding FTI and the penalties for unauthorized inspection or disclosure of FTI.

C. CRIMINAL JUSTICE INFORMATION

I understand the following:

1. I may have access to criminal justice information as defined in footnote 2 below, via the state network.
2. My access to this information is limited for the purpose(s) outlined in the agreement between the State Information Technology Services Division and the government agency providing the information.
3. Criminal history information and related information are particularly sensitive and may cause great harm if misused.
4. Misuse of the system by accessing it without authorization, exceeding the authorization, using the system improperly, or using, disseminating or re-disseminating criminal justice information without authorization, may constitute a state crime, federal crime, or both.

D. OTHER CONFIDENTIAL INFORMATION

I understand that I may have access to other confidential information such as a person's first and last name, address, telephone number, email address, social security number, bank and credit card information, health information, and other unique identifying information about a person. This information is confidential and may not be used or disclosed without proper authorization from my supervisor.

I have read and understand this Acknowledgement. A violation of the above terms and conditions may result in disciplinary action up to and including termination from employment.

Signed _____
Date _____

1 **FTI (IRS Code) -** A taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies over assessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing.

2 **CJIS Information -** information considered to be criminal justice in nature to include images, files, records, and intelligence information. FBI CJIS information is information derived from state or Federal CJIS systems.

NOTE: This form will be signed by each **(add Agency)** *employee with elevated privileges on an annual basis.*